UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,296	09/10/2003	Catherine M. Keene	AGIL-00501	5469

7590 12/09/2005

David R. Stevens
Stevens Law Group
P.O. Box 1667
San Jose, CA 95109

EXAMINER	
PHAM, HUNG Q	

ART UNIT	PAPER NUMBER
2168	

DATE MAILED: 12/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/660,296	KEENE ET AL.	
	Examiner	Art Unit	
	HUNG Q. PHAM	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 13-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 13-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 October 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/11/2005 has been entered.

Response to Arguments

- Applicants have been amended claims 1-7 and 13-15. The previous objection to claims 13 and 15 and rejection under 35 U.S.C. § 112 have been withdrawn.

- Claims 1, 7 and 13-15 have been rejected under 35 U.S.C. § 112, first paragraph. However, there is no response to this rejection in the amendment filed on 09/16/2005. Therefore, the rejection of claims 1, 7 and 13-15 under 35 U.S.C. § 112, first paragraph, is maintained.

- In response to applicant's argument with respect to claim 1 that the references fail to show certain features of applicant's invention as in page 14 and the last paragraph of page 16, it is noted that the features upon which applicant relies (i.e.,

identifying a user to have access to the object, verifying a user's user privilege access criteria including extracting the user's user identification from the object request, verifying first in cache memory and if not in cache then in main memory the user's user identification, and *the security system of Mukherjee ... not in a multi-vendor system where the multiple vendors are frequently competitors*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

- Applicant's arguments as in pages 14 with respect to the features of claims 7 and 13-15 have been considered but are moot in view of the new ground(s) of rejection.

Drawings

As set forth in the previous action, the drawing of FIG. 8 is objected to because the top margin of FIG. 8 does not have a top margin of at least 2.5 cm. (1 inch).

Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement

sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

- As set forth by 37 C.F.R § 1.75 (i), *where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation.* Claims 1, 7 and 13-15 are objected to because there is no line indentation to separate the elements of the claim. Appropriate correction is required.

- Claim 7 is objected to because of the following informalities:

(1) At lines 3 and 4 of claim 7, a comma was used between two distinct steps (should be replaced by a semicolon).

storing the object, the object comprising distinguishable groups of data, establishing access criteria

(2) The clause *including identifying separate groups of information...* modifies the clause *each group of data* without a coordinator, e.g., "and":

wherein each group of data having an associated user privilege (and) ***including identifying separate groups of information to which the user may have access criteria for access to the groups of data***

(3) The terms *privilege access criteria, access criteria* and *user privilege access criteria* are interchangeable. To have a consistency of terminology, either *privilege access criteria, access criteria* or *user privilege access criteria* is used in the claim.

Appropriate correction is required.

- Claim 13 is objected to because of the following informalities:

(1) At line 8 of claim 13, a comma and a semicolon were used between two distinct steps (the comma should be deleted).

distinguishable groups of data,; computer readable code means for identifying a user to

(2) At line 15 of claim 13, two semicolons were used between two distinct steps (one should be deleted).

information and user privileges;; computer readable code means for receiving an object

(3) The terms *privilege access criteria, access criteria* and *user privilege access criteria* are interchangeable. To have a consistency of terminology, either *privilege access criteria, access criteria* or *user privilege access criteria* is used in the claim.

Appropriate correction is required.

- Claim 14 is objected to because of the following informalities:

The terms *privilege access criteria*, *access criteria* and *user privilege access criteria* are interchangeable. To have a consistency of terminology, either *privilege access criteria*, *access criteria* or *user privilege access criteria* is used in the claim.

Appropriate correction is required.

- Claims 7 and 13-15 are objected to because of the following informalities: *searching first in cache and if not found in memory then in main memory* (cache should be used instead of memory to have a consistency of terminology). Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 1, 7, 13-15 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As in claim 1, the claimed ***a cache memory for storing user access criteria*** was not described in the specification (as in FIG. 4, only a cache memory 402 is specified, and this cache is for storing user ID's as claimed).

As in claim 7, the claimed ***user privilege including identifying separate groups of information to which the user may have access criteria for access to the groups of data*** was not described in the specification.

As in claims 7 and 13-15, the claimed ***verifying a user's user privilege access criteria including ... verifying first in cache memory and if not in cache then in main memory the user's user identification***, and ***searching first in caches and if not found in memory then in main memory and retrieving the data requested*** was not described in the specification.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 13 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 13,

At lines 12 and 13, the clause ***including identifying separate groups of information to which the user may have access criteria for access to the groups of data*** references to some other items in the claim. It is unclear what item is being referenced.

Regarding claim 15,

From line 8 to line 10, the clause ***including identifying separate groups of information to which the user may have access criteria for access to the groups of data*** references to some other items in the claim. It is unclear what item is being referenced.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claim 1, 2, 6 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mukherjee et al. [USP 5,317,729] in view of Sadovsky [USP 5,689,638].

Regarding claim 1, Mukherjee teaches a system and method for providing the transfer and control access to a version of an object and associated information. The Mukherjee system and method comprises:

means for establishing an object (BILL OF MATERIAL or BOM is an object created by a design engineer, Col. 4, Lines 26-31 and 48-51),

the object comprising distinguishable groups of data (BOM comprises a plurality of rows with different data as distinguishable groups of data, FIG. 4),

each group of data having associated access criteria for access to the groups of data (each row has associated SECURITY LEVEL as access criteria for access to group of data, Col. 5, Line 55-Col. 6, Line 22);

a database for storing the object and associated information (FIG. 1, RELATIONAL DATABASE 40 storing BOM and associated information, e.g., ENGINEERING CHANGE NOTICES...);

means for establishing access criteria (SECURITY LEVEL as access criteria is established by DATA ACCESS AUTHORIZATION TABLE as in FIG. 3),

wherein each group of data has a user privilege associated with it for identifying separate groups of information to which user may have access to the groups of data (VIEW ID as user

privilege, e.g., ENGL associated with group of data with INSERT SEQUENCE 6001, LOC1 associated with group of data with INSERT SEQUENCE 4001 as in BOM of FIG. 9, Col. 6, Lines 32-36), and

setting a user's ID including defining which users are allowed to access the object and associated information and user privileges associated with the object and information (DESIGN ENGINEERING, MANUFACTURING ENGINEERING... as user IDs to control access to different BOM version, and ENGINEERING CHANGE NOTICES, ITEM ENGINEERING DATA as associated information are defined, view ID as *user privileges associated with the object and information*);

a central processing unit (CPU) for controlling the access to the database in accordance with the access criteria; a memory for storing software code for controlling the operation of the CPU (FIG. 1, PROCESSOR 30, and VERSION CONTROL COMPUTER PROGRAM 20 implies a memory for embedding the program, Col. 4, Lines 12-16 and 64-67);

access application code, stored in the memory and executable by the CPU (FIG. 11),

the application code being responsive to the user ID and user access criteria associated with the groups of data contained within an object and to predetermined privileges for allowing controlled access to individual groups of data contained within the object by an individual user according to the user's access privileges (FIG. 11, Col. 9, Lines 22-29);

thereby transmitting a redacted object to a user wherein transmitting a redacted object includes sending an electronic object to the user that contains the groups of information to which the user has access to and that excludes groups of information to which the user does not have access (by using the application program as in FIG. 11, PRODUCTION PLANNING associated with SECURITY LEVEL 3, for example, can retrieve a BOM of FIG. 10 with rows

corresponding only to INSERT SEQUENCE 4001, the BOM of only INSERT SEQUENCE 4001 is a redacted BOM or object, because the original BOM includes SEQUENCE 6001 and 4001, wherein rows of SEQUENCE 6001 as information group to which the user does not have access are excluded, FIG. 11, Col. 6, Lines 32-41).

The missing in Mukherjee teaching is ***a cache memory for storing user ID's***; and ***a cache memory for storing user access criteria.***

However, cache is a conventional memory and frequently used data are stored in cache, each time the processor references an address in memory, cache is checked first for quick access. Sadovsky discloses the technique of storing authentication data in cache for quick access (Sadovsky, Abstract).

It would have been obvious for one of ordinary skill in the art at the time the invention was made to store user ID and access criteria as disclosed at Mukherjee FIG. 3 in cache, and by storing authentication data in cache, the verifying process will be faster.

Regarding claim 2, Mukherjee and Sadovsky, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Mukherjee further discloses ***access includes the ability of a user to read the contents of a requested object*** (Col. 8, Line 61-Col. 9, Line 21).

Regarding claim 6, Mukherjee and Sadovsky, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Mukherjee further discloses the claimed ***the access is determined by a business relationship to produce products and defined by the host according to the need of information in a product chain*** (FIG. 3 and 4).

Regarding claim 16, Mukherjee and Sadovsky, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Mukherjee further discloses ***means for sending an electronic object to the user that contains the groups of information to which the user has access to and that excludes groups of information to which the user does not have access*** (by using the application program as in FIG. 11, PRODUCTION PLANNING associated with SECURITY LEVEL 3, for example, can retrieve a BOM of FIG. 10 with rows corresponding only to INSERT SEQUENCE 4001, the BOM of only INSERT SEQUENCE 4001 is a redacted BOM or object, because the original BOM includes SEQUENCE 6001 and 4001, wherein rows of SEQUENCE 6001 as information group to which the user does not have access are excluded, FIG. 11, Col. 6, Lines 32-41).

Claim 7 and 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mukherjee et al. [USP 5,317,729] in view of Hayes et al. [WO 95/14266] and Sadovsky [USP 5,689,638].

Regarding claim 7, Mukherjee teaches a system and method for providing the transfer and control access to a version of an object and associated information. The Mukherjee system and method comprises:

establishing an object (BILL OF MATERIAL or BOM is an object created by a design engineer, Col. 4, Lines 26-31 and 48-51)

including loading information into the object into separate groups having separate privilege access criteria (each row in BOM as a *group* has loaded information and associated SECURITY LEVEL as *privilege access criteria*, Col. 5, Line 55-Col. 6, Line 22);

storing the object (FIG. 1, RELATIONAL DATABASE 40 storing BOM and associated information, e.g., ENGINEERING CHANGE NOTICES...),

the object comprising distinguishable groups of data (BOM comprises a plurality of rows with different data as distinguishable groups of data, FIG. 4);

establishing access criteria (SECURITY LEVEL as access criteria is established by DATA ACCESS AUTHORIZATION TABLE as in FIG. 3),

wherein each group of data

having an associated user privilege (*each group of data*, e.g., a row of BOM as in FIG. 4, *having an associated user privilege*, e.g., view ID)

including identifying separate groups of information to which the user may have access criteria for access to the groups of data (*separate groups of information to which the user may have access criteria for access to the groups of data*, e.g., ITEM ENGINERRING DATA, EC AFECTED ITEM are *identified* by SECURITY LEVEL as in FIG. 4 where an engineer at the SECURITY LEVEL has access);

setting a use's ID including defining which users are allowed to access the object and associated information and user privileges (FIG. 3 performs *setting a use's ID*, wherein DESIGN ENGINEERING, MANUFACTURING ENGINEERING... as *which user are allowed to access the object and associated information and user privileges*, e.g., BOM as *object*, information in BOM as *associated information*, view ID as *user privileges* as in FIG. 4);

controlling the access to the database using a central processing unit (CPU) according to the access criteria (FIG. 1, PROCESSOR 30, and VERSION CONTROL COMPUTER PROGRAM 20, Col. 4, Lines 12-16 and 64-67);

storing software code for controlling the operation of the CPU in memory (FIG. 1, PROCESSOR 30, and VERSION CONTROL COMPUTER PROGRAM 20 implies a memory for embedding the program, Col. 4, Lines 12-16 and 64-67);

verifying a user's user privilege access criteria (Col. 9, Lines 51-68);

verifying in main memory the user's user identification (Access control is specified as in FIG. 3. As further disclosed by Mukherjee at Col. 9, Lines 51-68, the "release only" option gives the engineer at the controlling location visibility to the latest level of EC data that has been sent out to remote locations or released to manufacturing. The teaching as discussed implies a user, either a design engineering or manufacturing engineering, at the controlling location has been verified to get access to the "release" status);

identifying the groups of data to which the user has access and privileges with respect thereto thereby allowing controlled access to individual groups of data contained within the object by an individual user according to the user's privileges in response to the access criteria associated with the groups of data contained within an object and to predetermined privileges upon verification of user ID and user privileges (by entering ITEM NUMBER and BOM name as in FIG. 11, in response to SECURITY LEVEL and

view ID as *access criteria* and *predetermined privileges* associated with rows of data within BOM, groups of data to which design or manufacturing engineers have access and privileges are identified by SECURITY LEVEL and VIEW ID in each BOM rows, e.g., FIG. 10, and that design or manufacturing engineers are allowed to view the BOM rows according to view ID, Col. 5, Lines 64-68, Col. 9, Lines 21-39)

searching in main memory and retrieving the data requested according to the user's access criteria and transmitting a redacted object to the user, wherein transmitting a redacted object includes sending an electronic object to the use that contains the groups of information to which the user has access to and that excludes groups of information to which the user does not have access (by using the application program as in FIG. 11, PRODUCTION PLANNING associated with SECURITY LEVEL 3, for example, can search in memory and retrieve a BOM of FIG. 10 with rows corresponding only to INSERT SEQUENCE 4001, the BOM of only INSERT SEQUENCE 4001 is a redacted BOM or object, because the original BOM includes SEQUENCE 6001 and 4001, wherein rows of SEQUENCE 6001 as information group to which the user does not have access are excluded, FIG. 11, Col. 6, Lines 32-41).

The missing in Mukherjee teaching is the steps of ***extracting the user's user identification from the object request*** that included in verifying process, ***verifying first in cache memory the user's user identification***, and ***searching first in cache and*** for retrieving the data requested.

Hayes teaches the steps of ***extracting the user's user identification from the object request*** (Hayes, FIG. 1).

Sadovsky teaches the step of ***verifying first in cache memory the user's user identification*** (Sadovsky, Col. 7, Line 66-Col. 8, Line 10).

Cache is a conventional memory and frequently used data are stored in cache, each time the processor references an address in memory, cache is checked first for quick access (Computer Dictionary).

As taught by Mukherjee, access is controlled at location, e.g., a manufacturing engineering can only get access to his/her status level at his/her location (Mukherjee, Col. 9, Lines 51-68). By applying the technique ***extracting the user's user identification from the object request*** of as taught by Hayes, a manufacturing engineering can get access to a particular security level data at any location, e.g., production location, by combining user identification with a requested object.

By including a conventional cache and the technique of ***verifying first in cache memory the user's user identification*** as taught by Sadovsky, the processing time of retrieving data will be improved significantly.

Regarding claim 13, Mukherjee teaches a program for use with a computer system, a central unit and means coupled to the central processing unit for storing a database to automatically manage objects for viewing and marking an object having varying formats without the use of any originating application of a file to view the object (FIG. 1 and 11). The Mukherjee program comprises:

computer readable code means for establishing an object in a storage location (BILL OF MATERIAL or BOM is an object created by a design engineer, Col. 4, Lines 26-31 and 48-51, FIG. 1, RELATIONAL DATABASE 40 storing BOM)

including loading information into the object into separate groups having separate privilege access criteria (each row in BOM as a group has loaded information and associated SECURITY LEVEL as privilege access criteria, Col. 5, Line 55-Col. 6, Line 22);

storing the object (FIG. 1, RELATIONAL DATABASE 40 storing BOM and associated information, e.g., ENGINEERING CHANGE NOTICES...),

the object comprising distinguishable groups of data (BOM comprises a plurality of rows with different data as distinguishable groups of data, FIG. 4);

computer readable code means for identifying a user to have access to the object (Col. 5, Lines 51-54);

computer readable code means for establishing privilege access criteria that define the scope of access of the object for the user (SECURITY LEVELS as privilege access criteria is established by DATA ACCESS AUTHORIZATION TABLE as in FIG. 3),

whereby each group of data has an associated user privilege that define the scope of access of the object for the user (VIEW ID as user privilege, e.g., ENGL associated with group of data with INSERT SEQUENCE 6001, LOC1 associated with group of data with INSERT SEQUENCE 4001 as in BOM of FIG. 9, Col. 6, Lines 32-36)

including identifying separate groups of information to which the user may have access criteria for access to the groups of data (*separate groups of information to which the user may have access criteria for access to the groups of data*, e.g., ITEM ENGINERRING DATA, EC AFECTED ITEM are *identified* by SECURITY LEVEL as in FIG. 4 where an engineer at the SECURITY LEVEL has access);

setting a user's ID including defining which user are allowed to access to object and associated information and user privileges (FIG. 3 performs *setting a use's ID*, wherein DESIGN

ENGINEERING, MANUFACTURING ENGINEERING... as *which user are allowed to access the object and associated information and user privileges*, e.g., BOM as *object*, information in BOM as *associated information*, view ID as *user privileges* as in FIG. 4);

computer readable code means for receiving an object request by a user (FIG. 11);

computer readable code means verifying a user's user privilege access criteria (Col. 9, Lines 51-68);

verifying in main memory the user's user identification (Access control is specified as in FIG. 3. As further disclosed by Mukherjee at Col. 9, Lines 51-68, the "release only" option gives the engineer at the controlling location visibility to the latest level of EC data that has been sent out to remote locations or released to manufacturing. The teaching as discussed implies a user, either a design engineering or manufacturing engineering, at the controlling location has been verified to get access to the "release" status);

identifying the groups of data to which the user has access and privileges with respect thereto thereby allowing controlled access to individual groups of data contained within the object by an individual user according to the user's privileges in response to the access criteria associated with the groups of data contained within an object and to predetermined privileges upon verification of user ID and user privileges (by entering ITEM NUMBER and BOM name as in FIG. 11, in response to SECURITY LEVEL and view ID as *access criteria* and *predetermined privileges* associated with rows of data within BOM, groups of data to which design or manufacturing engineers have access and privileges are identified by SECURITY LEVEL and VIEW ID in each BOM rows, e.g., FIG. 10, and that design or manufacturing engineers are allowed to view the BOM rows according to view ID, Col. 5, Lines 64-68, Col. 9, Lines 21-39)

searching in main memory and retrieving the data requested according to the user's access criteria; and computer readable code means for transmitting a redacted document according to the user's user privilege access criteria including sending an electronic object to the user that contains the groups of information to which the user has access to and that excludes groups of information to which the user does not have access (by using the application program as in FIG. 11, PRODUCTION PLANNING associated with SECURITY LEVEL 3, for example, can search in memory and retrieve a BOM of FIG. 10 with rows corresponding only to INSERT SEQUENCE 4001, the BOM of only INSERT SEQUENCE 4001 is a redacted BOM or object, because the original BOM includes SEQUENCE 6001 and 4001, wherein rows of SEQUENCE 6001 as information group to which the user does not have access are excluded, FIG. 11, Col. 6, Lines 32-41).

The missing in Mukherjee teaching is the steps of *extracting the user's user identification from the object request* that included in verifying process, *verifying first in cache memory the user's user identification*, and *searching first in cache and* for retrieving the data requested.

Hayes teaches the steps of *extracting the user's user identification from the object request* (Hayes, FIG. 1).

Sadovsky teaches the step of *verifying first in cache memory the user's user identification* (Sadovsky, Col. 7, Line 66-Col. 8, Line 10).

Cache is a conventional memory and frequently used data are stored in cache, each time the processor references an address in memory, cache is checked first for quick access (Computer Dictionary).

As taught by Mukherjee, access is controlled at location, e.g., a manufacturing engineering can only get access to his/her status level at his/her location (Mukherjee,

Col. 9, Lines 51-68). By applying the technique *extracting the user's user identification from the object request* of as taught by Hayes, a manufacturing engineering can get access to a particular security level data at any location, e.g., production location, by combining user identification with a requested object.

By including a conventional cache and the technique of *verifying first in cache memory the user's user identification* as taught by Sadovsky, the processing time of retrieving data will be improved significantly.

Regarding claim 14, Mukherjee teaches a system and method for providing the transfer and control access to a version of an object and associated information. The Mukherjee system and method comprises:

a computer program storage device readable by a digital processing apparatus; a program stored on the program storage device and including instructions executable by the digital processing apparatus for controlling the apparatus to perform a method of managing documents for viewing and marking an object having varying formats (Col. 4, Lines 12-25) *without the use of any originating application of a file to view the object stored in the file* (objects are stored in a relational database but data is retrieved by an application program as in FIG. 1, not using SQL statement for retrieving), comprising:

establishing an object in a storage location (BILL OF MATERIAL or BOM is an object created by a design engineer, Col. 4, Lines 26-31 and 48-51, FIG. 1, RELATIONAL DATABASE 40 storing BOM)

including loading information into the object into separate groups having separate privilege access criteria (each row in BOM as a group has loaded information and associated SECURITY LEVEL as privilege access criteria, Col. 5, Line 55-Col. 6, Line 22);

storing the object (FIG. 1, RELATIONAL DATABASE 40 storing BOM and associated information, e.g., ENGINEERING CHANGE NOTICES...),

the object comprising distinguishable groups of data (BOM comprises a plurality of rows with different data as distinguishable groups of data, FIG. 4);

identifying a user to have access to the object (Col. 5, Lines 51-54);

establishing privilege access criteria that define the scope of access of the object for the user (SECURITY LEVELS as privilege access criteria is established by DATA ACCESS AUTHORIZATION TABLE as in FIG. 3);

receiving an object request by a user (FIG. 11);

verifying a user's user privilege access criteria (Col. 9, Lines 51-68);

verifying in main memory the user's user identification (Access control is specified as in FIG. 3. As further disclosed by Mukherjee at Col. 9, Lines 51-68, the "release only" option gives the engineer at the controlling location visibility to the latest level of EC data that has been sent out to remote locations or released to manufacturing. The teaching as discussed implies a user, either a design engineering or manufacturing engineering, at the controlling location has been verified to get access to the "release" status);

identifying the groups of data to which the user has access and privileges with respect thereto thereby allowing controlled access to individual groups of data contained within the object by an individual user according to the user's privileges in response to the access criteria associated with the groups of data contained within an object and to predetermined privileges upon verification of user ID and user privileges (by entering ITEM NUMBER and BOM name as in FIG. 11, in response to SECURITY LEVEL and view ID as *access criteria* and *predetermined privileges* associated with rows of data within BOM, groups of data to which design or manufacturing engineers have access and privileges

are identified by SECURITY LEVEL and VIEW ID in each BOM rows, e.g., FIG. 10, and that design or manufacturing engineers are allowed to view the BOM rows according to view ID, Col. 5, Lines 64-68, Col. 9, Lines 21-39),

searching in main memory and retrieving the data requested according to the user's access criteria; and transmitting a redacted object according to the user's user privilege access criteria including sending an electronic object to the user that contains the groups of information to which the user has access to and that excludes groups of information to which the user does not have access (by using the application program as in FIG. 11, PRODUCTION PLANNING associated with SECURITY LEVEL 3, for example, can search in memory and retrieve a BOM of FIG. 10 with rows corresponding only to INSERT SEQUENCE 4001, the BOM of only INSERT SEQUENCE 4001 is a redacted BOM or object, because the original BOM includes SEQUENCE 6001 and 4001, wherein rows of SEQUENCE 6001 as information group to which the user does not have access are excluded, FIG. 11, Col. 6, Lines 32-41).

The missing in Mukherjee teaching is the steps of ***extracting the user's user identification from the object request*** that included in verifying process, ***verifying first in cache memory the user's user identification***, and ***searching first in cache and*** for retrieving the data requested.

Hayes teaches the steps of ***extracting the user's user identification from the object request*** (Hayes, FIG. 1).

Sadovsky teaches the step of ***verifying first in cache memory the user's user identification*** (Sadovsky, Col. 7, Line 66-Col. 8, Line 10).

Cache is a conventional memory and frequently used data are stored in cache, each time the processor references an address in memory, cache is checked first for quick access (Computer Dictionary).

As taught by Mukherjee, access is controlled at location, e.g., a manufacturing engineering can only get access to his/her status level at his/her location (Mukherjee, Col. 9, Lines 51-68). By applying the technique ***extracting the user's user identification from the object request*** of as taught by Hayes, a manufacturing engineering can get access to a particular security level data at any location, e.g., production location, by combining user identification with a requested object.

By including a conventional cache and the technique of ***verifying first in cache memory the user's user identification*** as taught by Sadovsky, the processing time of retrieving data will be improved significantly.

Regarding claim 15, Mukherjee teaches a method of securely transferring data between a source and an access destination in a computer server having a database for storing data pertaining to product information (Abstract and FIG. 1). The Mukherjee method comprising:

establishing an object in a storage location (BILL OF MATERIAL or BOM is an object created by a design engineer, Col. 4, Lines 26-31 and 48-51, FIG. 1, RELATIONAL DATABASE 40 storing BOM)

including loading information into the object into separate groups having separate privilege access criteria (each row in BOM as a group has loaded information and associated SECURITY LEVEL as privilege access criteria, Col. 5, Line 55-Col. 6, Line 22);

storing the object (FIG. 1, RELATIONAL DATABASE 40 storing BOM and associated information, e.g., ENGINEERING CHANGE NOTICES...),

the object comprising distinguishable groups of data (BOM comprises a plurality of rows with different data as distinguishable groups of data, FIG. 4);

identifying a user to have access to the object (Col. 5, Lines 51-54);

establishing access criteria (SECURITY LEVEL as access criteria is established by DATA ACCESS AUTHORIZATION TABLE as in FIG. 3),

wherein each group of data

has an associated user privilege that define the scope of access of the object for the user (*each group of data*, e.g., a row of BOM as in FIG. 4, *having an associated user privilege defining the scope of access of the object*, e.g., view ID)

including identifying separate groups of information to which the user may have access criteria for access to the groups of data (*separate groups of information to which the user may have access criteria for access to the groups of data*, e.g., ITEM ENGINERRING DATA, EC AFECTED ITEM are *identified* by SECURITY LEVEL as in FIG. 4 where an engineer at the SECURITY LEVEL has access);

setting a user's ID including defining which user are allowed to access to object and associated information and user privileges (FIG. 3 performs *setting a use's ID*, wherein DESIGN ENGINEERING, MANUFACTURING ENGINEERING... as *which user are allowed to access the object and associated information and user privileges*, e.g., BOM as *object*, information in BOM as *associated information*, view ID as *user privileges* as in FIG. 4);

receiving an object request by a user (FIG. 11);

verifying a user's user privilege access criteria (Col. 9, Lines 51-68);

verifying in main memory the user's user identification (Access control is specified as in FIG. 3. As further disclosed by Mukherjee at Col. 9, Lines 51-68, the "release only" option

gives the engineer at the controlling location visibility to the latest level of EC data that has been sent out to remote locations or released to manufacturing. The teaching as discussed implies a user, either a design engineering or manufacturing engineering, at the controlling location has been verified to get access to the "release" status);

identifying the groups of data to which the user has access and privileges with respect thereto thereby allowing controlled access to individual groups of data contained within the object by an individual user according to the user's privileges in response to the access criteria associated with the groups of data contained within an object and to predetermined privileges upon verification of user ID and user privileges (by entering ITEM NUMBER and BOM name as in FIG. 11, in response to SECURITY LEVEL and view ID as *access criteria* and *predetermined privileges* associated with rows of data within BOM, groups of data to which design or manufacturing engineers have access and privileges are identified by SECURITY LEVEL and VIEW ID in each BOM rows, e.g., FIG. 10, and that design or manufacturing engineers are allowed to view the BOM rows according to view ID, Col. 5, Lines 64-68, Col. 9, Lines 21-39);

searching in main memory and retrieving the data requested according to the user's access criteria and transmitting a redacted object to the user, wherein transmitting a redacted object includes sending an electronic object to the use that contains the groups of information to which the user has access to and that excludes groups of information to which the user does not have access (by using the application program as in FIG. 11, PRODUCTION PLANNING associated with SECURITY LEVEL 3, for example, can search in memory and retrieve a BOM of FIG. 10 with rows corresponding only to INSERT SEQUENCE 4001, the BOM of only INSERT SEQUENCE 4001 is a redacted BOM or object, because the original BOM includes SEQUENCE 6001 and 4001,

wherein rows of SEQUENCE 6001 as information group to which the user does not have access are excluded, FIG. 11, Col. 6, Lines 32-41).

The missing in Mukherjee teaching is the steps of ***extracting the user's user identification from the object request*** that included in verifying process, ***verifying first in cache memory the user's user identification***, and ***searching first in cache and*** for retrieving the data requested.

Hayes teaches the steps of ***extracting the user's user identification from the object request*** (Hayes, FIG. 1).

Sadovsky teaches the step of ***verifying first in cache memory the user's user identification*** (Sadovsky, Col. 7, Line 66-Col. 8, Line 10).

Cache is a conventional memory and frequently used data are stored in cache, each time the processor references an address in memory, cache is checked first for quick access (Computer Dictionary).

As taught by Mukherjee, access is controlled at location, e.g., a manufacturing engineering can only get access to his/her status level at his/her location (Mukherjee, Col. 9, Lines 51-68). By applying the technique ***extracting the user's user identification from the object request*** of as taught by Hayes, a manufacturing engineering can get access to a particular security level data at any location, e.g., production location, by combining user identification with a requested object.

By including a conventional cache and the technique of ***verifying first in cache memory the user's user identification*** as taught by Sadovsky, the processing time of retrieving data will be improved significantly.

Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mukherjee et al. [USP 5,317,729] and Sadovsky [USP 5,689,638], as applied to claim 2, and further in view of Koko et al. [USP 5,434,791].

Regarding claim 3, Mukherjee and Sadovsky, in combination, teach all of the claimed subject matter as discussed above with respect to claim 2, but does not explicitly teach ***the access includes the ability to modify the contents of the requested object***. Koko teaches a user interface for displaying a BOM and ***the ability to modify the contents of the requested object*** (Koko, Col. 28, Lines 5-10). It would have been obvious for one of ordinary skill in the art at the time the invention was made to include the ability to modify the contents of a retrieved BOM in order to correct information of a Bill of Material.

Regarding claim 4, Mukherjee, Sadovsky and Koko, in combination, teach all of the claimed subject matter as discussed above with respect to claim 3, Koko further discloses ***the ability to modify includes the ability to delete information contained in the requested object*** (Koko, Col. 28, Lines 5-10).

Regarding claim 5, Mukherjee, Sadovsky and Koko, in combination, teach all of the claimed subject matter as discussed above with respect to claim 3, Koko further discloses ***the ability to modify includes the ability to add data to the requested object*** (Koko, Col. 28, Lines 5-10).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HUNG Q. PHAM whose telephone number is 571-272-4040. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JEFFREY A. GAFFIN can be reached on 571-272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HUNG Q PHAM
Examiner
Art Unit 2168

December 6, 2005